21-11-2005

Investigating the relationship between Location-Based Services and National Security

Holly Tootell
University of Wollongong, holly@uow.edu.au

Investigating the relationship between Location-Based Services and National Security

Abstract

Public awareness of national security has increased significantly since September 11, 2001. Literature has discussed ways to respond or prevent breaches of National security with some of these methods employing information technologies, including Radio Frequency Identification (RFID) and Global Positioning System (GPS). Other studies have focused on the privacy impact the proposed solutions will have. This research examines the technologies under the umbrella of Location-Based Services (LBS). The preliminary findings of this research indicate that the broader notion of LBS is what needs to be focused on in order to understand the impact that they are having in the effort to ensure national security.

Disciplines

Physical Sciences and Mathematics

Publication Details

This article was originally published as: Tootell, H, Investigating the relationship between Location-Based Services and National Security, IEEE International Region 10 Conference (TENCON 2005), Melbourne, November 21-24 2005, 1-4.

Investigating the relationship between Location-Based Services and National Security

Holly Tootell, *Member, IEEE*

***Abstract*— Public awareness of national security has increased significantly since September 11, 2001. Literature has discussed ways to respond or prevent breaches of National security with some of these methods employing information technologies, including Radio Frequency Identification (RFID) and Global Positioning System (GPS). Other studies have focused on the privacy impact the proposed solutions will have. This research examines the technologies under the umbrella of Location-Based Services (LBS). The preliminary findings of this research indicate that the broader notion of LBS is what needs to be focused on in order to understand the impact that they are having in the effort to ensure national security.**

***Index Terms*—national security, location-based services.**

I. Introduction

Information Technology is acknowledged as one part of the solution to ensuring National security. Example technologies include Radio Frequency Identification (RFID) and Global Positioning System (GPS). Their advanced capabilities make them a favoured option in light of recent events of terrorist acts and natural disasters. These technologies are examples of a grouping of technologies called Location-Based Services (LBS). Their scope for use can range from immigration and visa control applications (through biometric identification on passports) to advanced home-detention functionality (RFID chips for movement tracking) [1]. Because of this flexibility in application there is a need to research the importance of them, and consequences of them, to national security.

In section 2, a definition of national security is established and is further described as the concept of event categorization is covered. LBS are described in section 3 bringing the focus of the paper to a synopsis of existing studies being conducted in two areas: technologies for national security protection, and privacy impact of national security. The paper is concluded with findings from research and the aims to be achieved in this continued work.

Manuscript received May 30, 2005.

H. Tootell is with University of Wollongong, Wollongong, NSW 2522 Australia, phone: +61 2 42215603; fax: +61 2 42214170; e-mail: holly@uow.edu.au.

II. National Security

A. Definitions

Homeland security is a neologism. It was found predominantly in US-based literature immediately following the events of September 11, culminating in the creation, by President Bush, of the Office of Homeland Security [2]. However, since 2001 the term has been gaining wider acceptance in Australia and other countries. The 'Australian Homeland Security Research Centre' is evidence of this. National security is related to homeland security and internal security as well as many other terms [3]. Two of the more common alternatives are listed below.

1) Border management: a term that describes how a country polices its borders
2) Counter terrorism: refers to the practices, tactics, and strategies that governments, militaries, and other groups adopt in order to fight terrorism.

Much literature refers to homeland security primarily with regard to terrorism, and often linked to the United States. In order to overcome these biases, the term 'National Security' has been chosen to encompass the wider meaning of the terms. For the purposes of this paper national security encompasses the following objectives:

a. Intelligence gathering and warning;
b. Border and transportation security;
c. Domestic counter-terrorism;
d. Protection of critical infrastructure;
e. Defending against outside attacks; and
f. Emergency preparedness and response. [4] [5]

B. Event Categorisations

National security can be examined in a number of ways. The first look is from a 'prevention vs. response' perspective. This refers to the distinction between actions that are undertaken to prevent an incident of interest from occurring and the [re]actions that take place once an incident of interest have occurred. The second perspective is to separate the initiation of the threat: whether is it domestic or international. Table 1 outlines sample events.

Preventive	Event	Threat
Intelligence and warning	Population, immigration control	Domestic/ International
Border and transportation security	Fleet management; security exclusion zones (air fields)	Domestic
Protecting critical	Creating	Domestic

infrastructures	redundancies	
Emergency preparedness	Research on natural disaster; warning systems	Domestic
Domestic counter-terrorism	Intelligence gathering	Domestic
Reactive	**Event**	
Emergency response	Natural disaster	Domestic
Defending outside attack	Terrorist activity	International

Table 1: Event Categorisation

III. Location-Based Services

Location-based services (LBS) are services that exploit knowledge about where an information device is located. The information device can be used to locate living and non-living entities. Location can be represented in a variety of ways and depending on the context LBS can utilize several technologies for knowing where an information device is geographically located. Global Positioning Satellites (GPS), Cell Identification, Broadband Satellite Network, Assisted GPS, Radio Frequency Identification (RFID) and Wireless Local Area Networks (WLAN) are examples of technologies used [6].

LBS have been used for many purposes, including: street directions, personalized marketing material dependent on location etc [6]. However they also provide an attractive solution to the more serious issue of National security. Their ability to transmit and identify location-specific information provides an invaluable resource for both preventative and reactive situations. The types of LBS applications that are being used as a response to National Security include: RFID (for disaster management, disease outbreaks, and secure access areas); biometric passports (for monitoring visitors to country), GPS devices for monitoring emergency response teams; monitoring of public health outbreaks and Mobile Stations (for emergency response).

Table 2 summarises actual events and the technology that was used to assist in the response. This is by no means an exhaustive list, but it does highlight the effectiveness of LBS in these situations.

Event	Location-Based Service
Border control	RFID – passive devices to denote 'cleared' vehicles GIS – unmanned aerial flight vehicles to provide image transmissions
Natural disaster	RFID – to manage victim identification GIS – to estimate damage and target areas
Terrorist attack	GPS – locating persons at attack site
Protection of Critical infrastructure	GPS – to monitor potential threats to major landmarks, buildings etc
Critical Health Outbreaks	RFID – to monitor patients, staff and visitors to hospitals during SARS Mobiles – updates of affected areas

Table 2: Event and LBS (adapted from Michael & Masters [5])

IV. National Security Research

Research being conducted in the area of national security and LBS can be separated into two categories: technology responses to resolving weaknesses in national security preparedness and communications; and privacy-based research that examine the responses of the public to the impact the proposed technologies will have on personal privacy.

A number of technology studies have researched the importance of wireless services in disaster recovery efforts [7] [8], particularly the uptake of commercial network provision as a viable alternative for the small market of public safety. They have identified that if primary communications infrastructure is damaged or destroyed, it is the mobile services that are the lifeline. In this instance though, the demands on the mobile services increases dramatically as they perform an increased number of functions. They are used to communicate with survivors, locate victims, coordinate search and rescue teams, and communicate between first responders. Chen [9] identified the area of Intelligence and security informatics (ISI) to describe the field of research aimed at developing advanced information technology solutions to homeland and national security applications.

Connolly [10], Chen [9] and Popp [11] identify the significance that IP location and internet content can make in making knowledge links for counter-terrorism responses. The use of satellite and radar as a means of alternative communication in the event of critical infrastructure problems is identified by Taggart [12] and Weber [13] respectively. In each of these studies, a particular application of the technology is examined, which allows for an in-depth understanding of the system to occur, but for disaster planning, it does not provide an over-arching view of the technology solutions being used together.

Privacy studies have identified LBS technologies as being perceived as a threat to privacy regardless of purpose [14]. They have also examined the change in public perception to information collection and management for the purpose of 'homeland' security [15] [16]. Halchin [17] [18] has examined the use of government websites by terrorist organizations as an aid to planning attacks. From this aspect, control and management of information is seen as critical to the fight to protect national security. However the counter argument to this is that by restricting access to online government information, potential terrorists are prevented from getting is, as are ordinary citizens. This reinforces the theme of this research that a 'price' is paid for national security.

It has been suggested that the issue of privacy is no different in this age of terrorism than at any other time [19]. Regan proposes that perception and reaction to privacy issues of national identification are stronger in the post-September 11 world, both for and against the argument for them. National ID is seen as a problem waiting for a solution (REF). Civil libertarians have protested strongly against systems of national identification in the US, UK and Australia for many years [20] [21] [22].

Seifert has written about the importance of information storage and collections in terms of infrastructure management [23] [24], related to this is the research by Raghu [25] that examines the need for collaborative decision making. This approach to national security research, although not from a technical or LBS perspective, is at least beginning to examine the problem holistically.

V. Findings and Future Directions

To align selected technologies currently being used to protect national security under the umbrella term of location-based services means that this research will be able to focus on the phenomena and consequences that are unique to it. To date the literature has not taken this integrated technology approach and by working from a technology-specific perspective, there is a risk of not realizing the overall significance of this technological response to national security.

Throughout the research on existing studies, there is a consistent theme of citizens needing to waive certain liberties or have reduced access to services in order for national security initiatives to be fully implemented. This is particularly noticeable in the privacy-based studies. The concept of this can be summarized as the figurative price that the average citizen is 'paying' for this increased level of national security.

Ng-Kruelle et. al. [26] have established the concept of 'Price of Convenience' as a means for understanding what a consumer is willing to give up of their privacy in order to gain a factor of convenience. This study examined the use of mobile devices. This research has established a direction in technology studies to look beyond the benefits of the tool itself and instead evaluate the impact it can have on the end user. By applying this to technical solutions to national security, the 'price' of security might begin to be understood.

VI. Conclusion and Future Directions

The outcome of this research means that governments will be able to evaluate proposed LBS solutions more effectively in terms of the impact they have on the population. Citizens too, will be able to better understand choices that are being put forward and evaluate options away from the emotion and rhetoric that has been seen to follow incidents of national security significance. Focusing particularly on the role of LBS, this work will go on to establish an evidence-based framework for understanding the 'price' people pay for national security when it is achieved using LBS.

References

[1] M. James, "Where are you now? Location detection systems and personal privacy," in *Science, Technology, Environment and Resources Section*, vol. 2005, Research Note no. 60 2003–04 ed, 2004.

[2] "Executive Order Establishing Office of Homeland Security," vol. 13228, 2001.

[3] H. C. Relyea, "Homeland security and information," *Government Information Quarterly*, vol. 19, pp. 213-223, 2002.

[4] L. Kun, "Technology and Policy Review for Homeland Security," *IEEE Engineering in Medicine and Biology Magazine*, vol. 23, pp. 30 - 44, 2004.

[5] K. Michael and A. Masters, "Realized and predicted applications of positioning technologies in defense intelligence," in *Applications of information systems to homeland security and defense*, H. Abbass and D. Ellam, Eds. USA: IDG, In Press.

[6] B. Rao and L. Minakakis, "Evolution of mobile location-based services," *Communications of the ACM*, vol. 46, pp. 61-65, 2003.

[7] K. Balachandran, K. C. Budka, T. L. Doumi, and J. H. Kang, "Third-generation wireless services for Homeland Security," *Bell Labs Technical Journal*, vol. 9, pp. 5-21, 2004.

[8] B. L. Malone, "Wireless search and rescue: Concepts for improved capabilities," *Bell Labs Technical Journal*, vol. 9, pp. 37-49, 2004.

[9] H. Chen, F.-Y. Wang, and D. Zeng, "Intelligence and security informatics for homeland security: information, communication, and transportation," *Intelligent Transportation Systems, IEEE Transactions on*, vol. 5, pp. 329-341, 2004.

[10] G. Connolly, A. Sachenko, and G. Markowsky, "Distributed traceroute approach to geographically locating IP devices," presented at Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 2003. Proceedings of the Second IEEE International Workshop on, 2003.

[11] R. Popp, T. Armour, T. Senator, and K. Numrych, "COUNTERING TERRORISM THROUGH INFORMATION TECHNOLOGY," *Association for Computing Machinery. Communications of the ACM*, vol. 47, pp. 36.

[12] D. Taggart, F. Bayuk, D. Ping, J. Hant, and M. Marshall, "Usage of commercial satellite systems for homeland security communications," presented at Aerospace Conference, 2003. Proceedings. 2003 IEEE, 2003.

[13] P. Weber, A. Premji, T. J. Nohara, and C. Krasnor, "Low-cost radar surveillance of inland waterways for homeland security applications," presented at Radar Conference, 2004. Proceedings of the IEEE, 2004.

[14] L. S. Strickland and L. E. Hunt, "Technology, security, and individual privacy: New tools, new threats, and new public perceptions," *Journal of the American Society for Information Science and Technology*, vol. 56, pp. 221-234, 2005.

[15] L. E. Feinberg, "FOIA, federal information policy, and information availability in a post-9/11 world," *Government Information Quarterly*, vol. 21, pp. 439-460, 2004.

[16] B. N. Meeks, "Conspicuous in their silence - Where are the voices defending the very fought-after privacy rights now threatened in the name of Homeland Security?," *Communications of the Acm*, vol. 46, pp. 15-16, 2003.

[17] L. E. Halchin, "Electronic government in the age of terrorism," *Government Information Quarterly*, vol. 19, pp. 243-254, 2002.

[18] L. E. Halchin, "Electronic government: Government capability and terrorist resource," *Government Information Quarterly*, vol. 21, pp. 406-419, 2004.

[19] P. M. Regan, "Old issues, new context: Privacy, information collection, and homeland security," *Government Information Quarterly*, vol. 21, pp. 481-497, 2004.

[20] R. Clarke, "Just Another Piece of Plastic for your Wallet: The 'Australia Card' Scheme," *Computers & Society*, vol. 18, pp. 7-21, 1988.

[21] Electronic Privacy Information Center, "EPIC Alert Volume 12.09," vol. 2005. Washington D.C.: Electronic Privacy Information Center (EPIC), 2005.

[22] London School of Economics and Political Science, "The Identity Project: An assessment of the UK Identity Cards Bill & its implications," London School of Economics and Political Science, London 2005.

[23] J. W. Seifert, "The effects of September 11, 2001, terrorist attacks on public and private information infrastructures: a preliminary assessment of lessons learned," *Government Information Quarterly*, vol. 19, pp. 225-242, 2002.

[24] J. W. Seifert and H. C. Relyea, "Do you know where your information is in the homeland security era?," *Government Information Quarterly*, vol. 21, pp. 399-405, 2004.

[25] T. S. Raghu, R. Ramesh, and A. B. Whinston, "Addressing the homeland security problem: A collaborative decision-making framework," in *Intelligence and Security Informatics, Proceedings*, vol. 2665, *Lecture Notes in Computer Science*, 2003, pp. 249-265.

[26] G. Ng-Kruelle, S. Paul, D. Rebne, and J. F. Hampe, "Price of Convenience: Privacy and Mobile Commerce," *Quarterly Journal of Electronic Commerce*, vol. 3, pp. 273 - 285, 2002.